

On cohomology groups H^1 of G –modules of finite type over cyclic groups

Derong Qiu *

(School of Mathematical Sciences, Capital Normal University,
Beijing 100048, P.R.China)

Abstract Let G be a cyclic group, in this paper, we study the Herbrand quotient and 1–th cohomology group on finitely generated G –modules in some cases. When G is of order 2, the order of the cohomology group is explicitly related to some invariants, and this relation is used to study unit groups over quadratic extensions of number fields. We also give some applications on Pell equations and class number of number fields.

Keywords: cohomology group, Herbrand quotient, unit group, number field, Pell equation

2000 Mathematics Subject Classification: 11R11; 11R27; 11R29

1. Introduction

The 1–th cohomology group $H^1(G, A)$ and the Herbrand quotient $h(G, A)$ for a G –module A are very useful for studying arithmetic when A is an arithmetic object, e.g., A is related to elliptic curves or number fields. However, their calculation are usually not easy, even when G is a group of order 2.

Let G be a cyclic group of order n with a generator σ , and let $(A, +)$ be a

* E-mail: derong@mail.cnu.edu.cn, derongqiu@gmail.com

finitely generated abelian group, we denote $r(A) = \text{rank}(A)$. We assume that A is a G -module. Throughout this paper, for a set S , we denote its cardinal by $\sharp S$. For an arbitrary abelian group B and a positive integer m , we denote $mB = \{mb : b \in B\}$ and $B[m] = \{b \in B : mb = 0\}$. For a G -module A , one has the following Tate cohomology groups: $\widehat{H}^i(G, A) = H^i(G, A)$ if $i \geq 1$; $\widehat{H}^0(G, A) = A^G/N_G A$, where $N_G = \sum_{\tau \in G} \tau \in \mathbb{Z}[G]$, and $\mathbb{Z}[G]$ is the group algebra of G over \mathbb{Z} .

Since G is a finite cyclic group, $\widehat{H}^{-1}(G, A) = H^1(G, A)$. The Herbrand quotient of the G -module A is $h(G, A) = \frac{\sharp \widehat{H}^0(G, A)}{\sharp H^1(G, A)}$ (see [AW] and [Se]).

For the Herbrand quotient and the 1-th cohomology group of a G -module A , we have

Proposition 1. Let G be a finite cyclic group, and A be a G -module. If there exists a G -submodule B of finite index in A which is a finitely generated free abelian group containing a G -invariant \mathbb{Z} -basis $X = \{x_1, \dots, x_r\}$ (i.e., $\tau X \subset X$ for all $\tau \in G$, or in other words, X is a G -set). Then

$$h(G, A) = \prod_{x \in X/G} \sharp G_x, \quad \text{and} \quad \sharp H^1(G, A) = \frac{(A^G : N_G A)}{\prod_{x \in X/G} \sharp G_x},$$

where $G_x = \{\tau \in G : \tau x = x\}$ is the stabilizer of x .

The proof will be given in Section 2 (see Proposition 2.1 in the following).

When $G = \langle \sigma \rangle$ is of order 2, for a G -module A which is a finitely generated abelian group, we simply denote $NA = (1 + \sigma)A = \{a + \sigma a : a \in A\}$, $N^-A = (1 - \sigma)A = \{a - \sigma a : a \in A\}$, $A^+ = A^G$, $r_+(A) = \text{rank}(A^+)$, and $r_-(A) = \text{rank}(A^-)$, where $A^- = \{a \in A : \sigma a = -a\}$. Obviously, $r(A) = r_+(A) + r_-(A)$, $A^+[2] = A^+ \cap A^- = A^-[2]$, $(A : A^+ + A^-) = (N^-A : 2A^-) = (NA : 2A^+)$.

Proposition 2. Let G be a group of order 2, and A be a G -module. If A is a finitely generated abelian group. Then

$$\begin{aligned}\sharp H^1(G, A) &= \frac{2^{r_-(A)} \cdot \sharp A^+[2]}{(A : A^+ + A^-)} = \frac{2^{r_-(A)} \cdot \sharp A^+[2]}{(NA : 2A^+)} \\ &= 2^{r_-(A) - r_+(A)} \cdot (A^+ : NA) = 2^{r(A) - 2r_+(A)} \cdot (A^+ : NA),\end{aligned}$$

$$\text{and } h(G, A) = 2^{2r_+(A) - r(A)}.$$

In particular, if $r_+(A) = 0$ and $A^+[2] = \{O\}$, then $A = A^+ + A^-$ and $\sharp H^1(G, A) = 2^{r_-(A)} = 2^{r(A)}$.

Proof. This is a consequence of the Theorem on Herbrand quotient (see [AW]), for the detail, see the proof of Theorem 1.5 of [Q] on a special case. \square

Remark. For the case that G is a group of order 2, the result in Prop.2 is unconditional, and more explicit than the one in Prop.1 above. For a cyclic group G of order bigger than 2, at present, by the same way as in Prop.2 above, we only has a relatively crude result as follows,

$$\begin{aligned}\sharp H^1(G, A) &= \frac{({}_NA : (1 - \sigma)({}_NA))}{(NA : n \cdot A^G)}, \\ (NA : n \cdot A^G) &= (A : A^G + {}_NA) = ((1 - \sigma)A : (1 - \sigma)({}_NA)),\end{aligned}$$

where the G -module $(A, +)$ is a finitely generated abelian group, $N = N_G \in \mathbb{Z}[G]$ as above, ${}_NA = \{a \in A : Na = 0\}$, $NA = \{Na : a \in A\}$.

The proof of Proposition 1 (see Proposition 2.1 below) is given in Section 2, and some examples are given there. In Section 3, we apply the formula in Prop.2 above to study unit groups over quadratic extensions of number fields (see Cor.3.1 below), from which we give different proofs for some known theorems about number

fields (see the proofs of Thm.3.2 and Thm.3.5 below), as well as some applications of Pell equations, units in CM number fields and class number of number fields (see Prop.3.3, Prop.3.4 and Prop.3.8 below).

2. H^1 and Herbrand quotient

Let G be a group, and X be a G -set. For each $x \in X$, the G -orbit of x is $\mathcal{O}(x) = \{\tau x : \tau \in G\}$, and the stabilizer of x , denoted by G_x , is the subgroup $G_x = \{\tau \in G : \tau x = x\}$. If X is finite, then $\sharp \mathcal{O}(x) = (G : G_x)$, the index of G_x in G . Moreover, the number N of G -orbits of X is given by the following formula: $N = \frac{1}{\sharp G} \cdot \sum_{\tau \in G} F(\tau)$, where for each $\tau \in G$, $F(\tau) = \sharp\{x \in X : \tau x = x\}$ (see [Ro, pp. 56~59]). In the following, we denote the set of G -orbits of X by X/G , and we write $X/G = \{x_1, \dots, x_r\}$ if each x_i is a representative in a G -orbit, and x_1, \dots, x_r represent all distinct G -orbits of X .

Now we come to prove the Proposition 1 above, that is, the following result.

Proposition 2.1. Let G be a finite cyclic group, and A be a G -module. If there exists a G -submodule B of finite index in A which is a finitely generated free abelian group containing a G -invariant \mathbb{Z} -basis $X = \{x_1, \dots, x_r\}$ (i.e., $\tau X \subset X$ for all $\tau \in G$, or in other words, X is a G -set). Then

$$h(G, A) = \prod_{x \in X/G} \sharp G_x, \quad \text{and} \quad \sharp H^1(G, A) = \frac{(A^G : N_G A)}{\prod_{x \in X/G} \sharp G_x},$$

where $G_x = \{\tau \in G : \tau x = x\}$ is the stabilizer of x .

Proof. From the exact sequence of G -modules $0 \rightarrow B \rightarrow A \rightarrow A/B \rightarrow 0$, by Herbrand's theorem (see e.g., [AW, p.109]), $h(G, A) = h(G, B) \cdot h(G, A/B)$. By assumption, A/B is finite, so $h(G, A/B) = 1$, and then $h(G, A) = h(G, B)$. So we

only need to work out $h(G, B)$.

For each $x \in X/G$, its G -orbit is $\mathcal{O}(x) = \{\tau x : \tau \in G/G_x\}$. Let $B(x) = \bigoplus_{\tau \in G/G_x} \mathbb{Z}\tau x$, then obviously, $B(x)$ is a G -submodule of B , and $B = \bigoplus_{x \in X/G} B(x)$ as G -modules. Note that $\mathbb{Z}x$ is a trivial G_x -module, and $B(x) = \bigoplus_{\tau \in G/G_x} \tau(\mathbb{Z}x) = \text{Ind}_{G_x}^G(\mathbb{Z}x)$, that is, $B(x)$ is the induced G -module by the G_x -module $\mathbb{Z}x$ (see [Br, p.67], [Neu, pp.10,11]). So by Shapiro's lemma (see [Br, p.136], [Neu, p.11]), we have $\widehat{H}^i(G, B(x)) = \widehat{H}^i(G_x, \mathbb{Z}x)$ ($i = 0, -1$). Hence $h(G, B(x)) = h(G_x, \mathbb{Z}x) = \sharp G_x$, the last equality follows easily from the fact that $\mathbb{Z}x$ is a trivial G_x -module. Therefore, by Herbrand's theorem,

$$h(G, B) = h(G, \bigoplus_{x \in X/G} B(x)) = \prod_{x \in X/G} h(G, B(x)) = \prod_{x \in X/G} \sharp G_x,$$

hence $h(G, A) = \prod_{x \in X/G} \sharp G_x$. Moreover, by definition, $\widehat{H}^0(G, A) = A^G/N_G A$, so $\sharp H^1(G, A) = \frac{\sharp \widehat{H}^0(G, A)}{h(G, A)} = \frac{(A^G : N_G A)}{\prod_{x \in X/G} \sharp G_x}$, and the proof is completed. \square

A question here is on what conditions does a G -module satisfy the assumption of the Proposition 2.1?

Example 2.2. For a finite cyclic group G , let X be a finite G -set. Let $A = \bigoplus_{x \in X} \mathbb{Z}x$ be the free abelian group with the \mathbb{Z} -basis X . Let G acts on A by the following way: $\tau(\sum_{x \in X} a_x x) = \sum_{x \in X} a_x \tau(x)$ ($\forall \tau \in G, x \in X, a_x \in \mathbb{Z}$). Then A is a G -module satisfies the assumption of the above Prop.2.1, so $h(G, A) = \prod_{x \in X/G} \sharp G_x$.

Example 2.3. Let K/\mathbb{Q} be a cyclic extension of degree n , its Galois group $G = \text{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle$ with a generator σ . We denote the integral ring of K by O_K . Assume that K has a normal integral basis, i.e., there is an element $\alpha \in O_K$ such that $\{\alpha, \sigma(\alpha), \dots, \sigma^{n-1}(\alpha)\}$ is an integral basis of K . Then O_K is a G -module

which is a finitely generated free abelian group containing a G -invariant \mathbb{Z} -basis $S = \{\alpha, \sigma(\alpha), \dots, \sigma^{n-1}(\alpha)\}$. Obviously, S is a transitive G -set, i.e., $\sharp(S/G) = 1$, so $S/G = \{\alpha\}$ and $G_\alpha = \{1\}$. Hence by Prop.2.1 above, the Herbrand quotient $h(G, O_K) = \sharp G_\alpha = 1$, and the order of the cohomology group $\sharp H^1(G, O_K) = \frac{(O_K^G : N_G O_K)}{1} = (\mathbb{Z} : \text{Tr}_{K/\mathbb{Q}} O_K)$. Here $N_G \alpha = \sum_{\tau \in G} \tau \alpha = \text{Tr}_{K/\mathbb{Q}} \alpha$ is the trace of α for every $\alpha \in O_K$.

Such cyclic number fields with a normal integral basis include the quadratic number fields K with odd discriminant $d(K)$ (i.e., $2 \nmid d(K)$), and the cyclotomic number fields $\mathbb{Q}(\zeta_n)$, where $n = p$ or $2p$, p is an odd prime number, ζ_n is a primitive n -th root of unity (see [Fe, p.27], [Nar, pp.165, 166]).

Example 2.4. Let A be an abelian variety defined over \mathbb{Q} , and let K be a cyclic number field with a cyclic Galois group $G = \text{Gal}(K/\mathbb{Q})$. By Mordell-Weil theorem, the set $A(K)$ of K -rational points of A is a finitely generated abelian group. Assume that $A(K)$ has a free \mathbb{Z} -basis $\{P_1, \dots, P_r\}$ ($r = \text{rank} A(K)$), such that $S = \{P_1, \dots, P_r\}$ is a G -set. Then $A(K)$ is a G -module satisfying the assumption of the above Prop.2.1. We may as well assume that $S/G = \{P_1, \dots, P_{r_1}\}$ with $r_1 \leq r$. For each $i \in \{1, \dots, r_1\}$, let $K_i = \mathbb{Q}(P_i)$ be the defined field of P_i . Then the stabilizer $G_{P_i} = \text{Gal}(K/K_i)$. So by Prop.2.1 above, the Herbrand quotient $h(G, A(K)) = \prod_{i=1}^{r_1} \sharp G_{P_i} = \prod_{i=1}^{r_1} \sharp \text{Gal}(K/K_i) = \prod_{i=1}^{r_1} [K : K_i]$, and $\sharp H^1(G, A(K)) = \frac{(A(K)^G : N_G A(K))}{\prod_{i=1}^{r_1} [K : K_i]} = \frac{(A(\mathbb{Q}) : N_{K/\mathbb{Q}} A(K))}{\prod_{i=1}^{r_1} [K : K_i]}$, in particular, $(A(\mathbb{Q}) : N_{K/\mathbb{Q}} A(K)) \geq \prod_{i=1}^{r_1} [K : K_i]$. If all $P_1, \dots, P_r \in A(\mathbb{Q})$, then $\text{rank} A(K) = \text{rank} A(\mathbb{Q})$, and $r_1 = r$, so $K_i = \mathbb{Q}$, $G_{P_i} = G$ for each $i = 1, \dots, r$. Hence in this case, $h(G, A(K)) = [K : \mathbb{Q}]^r = n^r$, $n = [K : \mathbb{Q}]$.

3. S -Unit groups

For the quadratic extension K/F of number fields with $K = F(\sqrt{D})$ for some $D \in F^* \setminus F^{*2}$, let $G = \text{Gal}(K/F) = \langle \sigma \rangle = \{1, \sigma\}$ be its Galois group with a generator σ . Let S_F be a finite set of primes of F , always containing all infinite primes of F . Let S_K be the set of primes of K lying above those in S_F . The group of S_K -units of K (resp. S_F -units of F) is denoted by $\mathbf{U}_{K,S}$ (resp. $\mathbf{U}_{F,S}$). In particular, if $S_F = S_\infty$ consists of all infinite primes of F , then we simply write $\mathbf{U}_{K,S_\infty} = \mathbf{U}_K$ (resp. $\mathbf{U}_{F,S_\infty} = \mathbf{U}_F$). By Dirichlet unit theorem (see [Neu], p.73), $\mathbf{U}_{K,S}$ and $\mathbf{U}_{F,S}$ are finitely generated abelian groups. For the ranks, We denote $r_{F,S} = \text{rank}(\mathbf{U}_{F,S})$ and $r_{K,S} = \text{rank}(\mathbf{U}_{K,S})$, We simply write $r_{F,S_\infty} = r_F$ and $r_{K,S_\infty} = r_K$. Then $\mathbf{U}_{F,S} \simeq \mathbf{W}_F \times \mathbb{Z}^{r_{F,S}}$, $\mathbf{U}_{K,S} \simeq \mathbf{W}_K \times \mathbb{Z}^{r_{K,S}}$, where \mathbf{W}_F and \mathbf{W}_K are the groups of roots of unity in F and K , respectively, $r_{F,S} = \#S_F - 1$, $r_{K,S} = \#S_K - 1$. Obviously, $\mathbf{U}_{K,S}$ is a G -module (see [Neu], p.74), and we have $\mathbf{U}_{K,S}^G = \mathbf{U}_{F,S}$. We also denote $\mathbf{U}_{K,S}^- = \{\alpha \in \mathbf{U}_{K,S} : N(\alpha) = 1\}$, $N\mathbf{U}_{K,S} = \mathbf{U}_{K,S}^{1+\sigma} = \{N(\alpha) : \alpha \in \mathbf{U}_{K,S}\}$, $N^-\mathbf{U}_{K,S} = \{\alpha/\sigma(\alpha) : \alpha \in \mathbf{U}_{K,S}\}$, where $N(\alpha) = N_{K/F}(\alpha) = \alpha \cdot \sigma(\alpha)$ is the norm of the element $\alpha \in K$ over F . We write $r_{K,S}^- = \text{rank}(\mathbf{U}_{K,S}^-)$, $r_{K,S_\infty}^- = r_K^-$, we also write simply $\mathbf{U}_{K,S_\infty}^- = \mathbf{U}_K^-$, $N\mathbf{U}_{K,S_\infty} = N\mathbf{U}_K$, $N^-\mathbf{U}_{K,S_\infty} = N^-\mathbf{U}_K$. Obviously, $\mathbf{U}_{F,S}[2] = \{\pm 1\}$, and $r_{K,S} = r_{F,S} + r_{K,S}^-$, i.e., $r_{K,S}^- = \#S_K - \#S_F$. Also $r(N\mathbf{U}_K) = r_F$.

Corollary 3.1. The order of the group $H^1(G, \mathbf{U}_{K,S})$ is

$$\begin{aligned} \#H^1(G, \mathbf{U}_{K,S}) &= \frac{2^{\#S_K - \#S_F + 1}}{(\mathbf{U}_{K,S} : \mathbf{U}_{F,S} \cdot \mathbf{U}_{K,S}^-)} = \frac{2^{\#S_K - \#S_F + 1}}{(N\mathbf{U}_{K,S} : \mathbf{U}_{F,S}^2)} \\ &= 2^{r_{K,S} - 2r_{F,S}} \cdot (\mathbf{U}_{F,S} : N\mathbf{U}_{K,S}) = 2^{\#S_K - 2\#S_F + 1} \cdot (\mathbf{U}_{F,S} : N\mathbf{U}_{K,S}). \end{aligned}$$

In particular, $(\mathbf{U}_{K,S} : \mathbf{U}_{F,S} \cdot \mathbf{U}_{K,S}^-) \mid 2^{\#S_K - \#S_F + 1}$ and $h(G, \mathbf{U}_{K,S}) = 2^{2\#S_F - \#S_K - 1}$.

Proof. Easily follows from Dirichlet unit theorem and the above Prop.2. \square

For the first application, we consider the known formula in the following Thm.3.2 for the Herbrand quotient of the relative quadratic extension, and gives a different proof of Theorem 1.3 on p.74 of [Neu] in this case.

Theorem 3.2 (see the Theorem 1.3 on p.74 of [Neu] for $n = [K : F] = 2$).

The Herbrand quotient

$$h(G, \mathbf{U}_{K,S}) = \frac{1}{2} \prod_{v \in S_F} n_v,$$

where n_v is the order of the decomposition group $G_w \subset G$ above v .

Proof. On the one hand, $S_F = S_r \sqcup S_i \sqcup S_s$, where $S_r = \{v \in S_F : v \text{ ramifies in } K\}$, $S_i = \{v \in S_F : v \text{ is inertia in } K\}$, $S_s = \{v \in S_F : v \text{ splits in } K\}$. So $\#S_F = \#S_r + \#S_i + \#S_s$ and $\#S_K = \#S_r + \#S_i + 2 \cdot \#S_s$. Also, $n_v = 1$ for $v \in S_s$, and $n_v = 2$ for $v \in S_r \cup S_i$, so $\prod_{v \in S_F} n_v = 2^{\#S_r + \#S_i} = 2^{2\#S_F - \#S_K}$. On the other hand, by Cor.3.1 above, $h(G, \mathbf{U}_{K,S}) = 2^{2\#S_F - \#S_K - 1}$, so the equality holds. \square

For the second application, we consider the case of real quadratic number fields.

Proposition 3.3. Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic number field with a square-free integer $D(> 0)$, and $G = \text{Gal}(K/\mathbb{Q})$. Let $\epsilon > 1$ be a fundamental unit of K . Then the following statements are equivalent:

- (1) $N(\epsilon) = -1$;
- (2) $\#H^1(G, \mathbf{U}_K) = 2$;
- (3) The Pell equation $x^2 - y^2D = -1$ in the case $D \equiv 2, 3 \pmod{4}$ (respectively, $(2x - y)^2 - y^2D = -4$ in the case $D \equiv 1 \pmod{4}$) has integral solutions.

Proof. By Dirichlet unit theorem, $\mathbf{U}_K = \langle -1 \rangle \times \langle \epsilon \rangle$, this ϵ is the unique

smallest unit greater than 1 (see [Wei], pp.238,239 and [JW], pp.82,83). Obviously, $N(\varepsilon) = \pm 1$, so $N\mathbf{U}_K \subset \{\pm 1\}$. It follows from the formula in the above Cor.3.1 that $\sharp H^1(G, \mathbf{U}_K) = 2(\mathbf{W}_{\mathbb{Q}} : N\mathbf{U}_K)$ with $\mathbf{W}_{\mathbb{Q}} = \{\pm 1\}$. So $\sharp H^1(G, \mathbf{U}_K) = 2$ if and only if $N\mathbf{U}_K = \{\pm 1\}$.

(1) \Leftrightarrow (2). If there is an element $\alpha \in \mathbf{U}_K$ such that $N\alpha = -1$, then since $\alpha = \pm \epsilon^m$ for some $m \in \mathbb{Z}$, we have $-1 = N(\epsilon)^m$, so m is odd and $N(\epsilon) = -1$. It follows from this that $N\mathbf{U}_K = \{\pm 1\}$ if and only if $N(\epsilon) = -1$. Hence $\sharp H^1(G, \mathbf{U}_K) = 2$ if and only if $N(\epsilon) = -1$.

(2) \Leftrightarrow (3). If $D \equiv 1 \pmod{4}$, then the integral ring $\mathcal{O}_K = \mathbb{Z}[\frac{-1+\sqrt{D}}{2}]$, each element of \mathcal{O}_K has the form $x + y \cdot \frac{-1+\sqrt{D}}{2}$, $x, y \in \mathbb{Z}$. So $N\mathbf{U}_K = \{\pm 1\}$ if and only if there are $x, y \in \mathbb{Z}$ such that $N(x + y \cdot \frac{-1+\sqrt{D}}{2}) = -1$, i.e., the equation $(2x - y)^2 - y^2 D = -4$ has integral solutions. Similar for the case $D \equiv 2, 3 \pmod{4}$, and the conclusion follows from the above discussion. \square

Note that the set of $D > 0$ for which the norm of the fundamental unit ϵ is -1 has not been determined (see [IR], P.192). Many interesting facts about Pell equation and its applications can be found in [JW].

For the third application, we consider the case of CM number fields.

Proposition 3.4. Let K be a CM number field (see [Wa], p.38), $F = K^+$ the real subfield, $[K : F] = 2$, and the Galois group $G = \text{Gal}(K/F) = \langle \sigma \rangle$ is generated by the complex conjugation σ on K . If $\sharp S_F = \sharp S_K$, for example, when every finite prime in S_F is ramified or inertia in K . Then

$$\sharp H^1(G, \mathbf{U}_{K,S}) = \frac{2}{(\mathbf{U}_{K,S} : \mathbf{U}_{F,S} \cdot \mathbf{W}_K)} = \frac{2}{(N\mathbf{U}_{K,S} : \mathbf{U}_{F,S}^2)} = 2^{-r_{K,S}} \cdot (\mathbf{U}_{F,S} : N\mathbf{U}_{K,S}),$$

in particular, $(\mathbf{U}_{K,S} : \mathbf{U}_{F,S} \cdot \mathbf{W}_K) = (N\mathbf{U}_{K,S} : \mathbf{U}_{F,S}^2) \mid 2$, $\sharp H^1(G, \mathbf{U}_{K,S}) \mid 2$, and

$$(\mathbf{U}_{F,S} : N\mathbf{U}_{K,S}) = 2^{r_{K,S}} \text{ or } 2^{r_{K,S}+1}.$$

Proof. Since $\text{rank}(\mathbf{U}_{K,S}^-) = r_{K,S} - r_{F,S} = \sharp S_K - \sharp S_F = 0$ and $F = K^+$ is totally real, it is easy to see that $\mathbf{U}_{K,S}^- = \mathbf{W}_K$. Note that $\sharp H^1(G, \mathbf{U}_{K,S})$ is a positive integer number, the conclusion follows directly from the formula of the above Cor.3.1. \square

From the above Prop.3.4, one can directly deduces the known index estimation of the unit groups of F, K , which gives a different proof of Theorem 4.12 on p.40 of [Wa].

Theorem 3.5 (see the Theorem 4.12 on p.40 of [Wa]). Let K and F be as in Prop 3.4 above. Then $(\mathbf{U}_K : \mathbf{U}_F \cdot \mathbf{W}_K) \mid 2$.

Proof. Take $S_F = S_\infty$, then $\mathbf{U}_{F,S} = \mathbf{U}_F$, $\mathbf{U}_{K,S} = \mathbf{U}_K$, and the condition of the above Prop.3.4 holds, so the conclusion follows. \square

Remark. For the cyclotomic field case, i.e., $K = \mathbb{Q}(\zeta_m)$ ($2 < m \in \mathbb{Z}$) and $F = K^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$, where ζ_m is a primitive m -th root of unity in the complex number field \mathbb{C} . If $m = p^t$ for some prime number p and integer $t \geq 1$, then $\mathbf{U}_K = \mathbf{U}_F \cdot \mathbf{W}_K$ (see [Wei], p.268 and [Wa], p.40). So by the above Prop.3.4 we have $\sharp H^1(G, \mathbf{U}_K) = 2$, $N\mathbf{U}_K = \mathbf{U}_F^2$, and $(\mathbf{U}_F : N\mathbf{U}_K) = 2^{r_K+1}$.

Now for the CM field K and its real subfield $F = K^+$ as above, let \mathbf{U}_F^+ be the set consisting of all totally positive units in F . It is easy to see that $\mathbf{U}_F^2 \subset N\mathbf{U}_K \subset \mathbf{U}_F^+ \subset \mathbf{U}_F$. Let $\phi : \mathbf{U}_K \rightarrow \mathbf{W}_K$, $\alpha \mapsto \alpha/\sigma(\alpha)$. Then from the proof of Theorem 4.12 in [Wa, p.40], we have

Corollary 3.6. (1) If $\phi(\mathbf{U}_K) = \mathbf{W}_K$, then $(\mathbf{U}_F : N\mathbf{U}_K) = 2^{r_K}$, $(N\mathbf{U}_K : \mathbf{U}_F^2) = (\mathbf{U}_K : \mathbf{U}_F \cdot \mathbf{W}_K) = 2$, and $\sharp H^1(G, \mathbf{U}_K) = 1$. In particular, $\mathbf{U}_F^+ \neq \mathbf{U}_F^2$;

(2) If $\phi(\mathbf{U}_K) = \mathbf{W}_K^2$, then $(\mathbf{U}_F : N\mathbf{U}_K) = 2^{r_K+1}$, $N\mathbf{U}_K = \mathbf{U}_F^2$, $\mathbf{U}_K = \mathbf{U}_F \cdot \mathbf{W}_K$, and $\sharp H^1(G, \mathbf{U}_K) = 2$.

For example, let $K = \mathbb{Q}(\zeta_m)$ and $F = K^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ be as above.

- (a) if m is not a prime power, then the conclusion (1) of Cor.3.6 holds.
- (b) if m is a prime power, then the conclusion (2) of Cor.3.6 holds.

Example 3.7. In this example, we let K, F be two real Galois extensions over \mathbb{Q} , $[K : F] = 2$, and $[F : \mathbb{Q}] = n$. The Galois group $G = \text{Gal}(K/F) = \{1, \sigma\}$ with a generator σ . Let $\mathbf{U}_K, \mathbf{U}_K^1, \mathbf{U}_K^+$ and \mathbf{U}_K^2 be the unit group, the subgroup of the units of norm 1, the subgroup of totally positive units and the subgroup of the unit squares, respectively, of K . Similar for the meaning of $\mathbf{U}_F, \mathbf{U}_F^1, \mathbf{U}_F^+$ and \mathbf{U}_F^2 . Let $\mathbf{U}_K^{+1} = \mathbf{U}_K^+ \cap \mathbf{U}_K^1$, $\mathbf{U}_K^{1,2} = \mathbf{U}_K^1 \cap \mathbf{U}_K^2$, $r_K^{+1} = \text{rank}(\mathbf{U}_K^{+1})$, $r_K^{1,2} = \text{rank}(\mathbf{U}_K^{1,2})$, $r_K^1 = \text{rank}(\mathbf{U}_K^1)$, $r_F^1 = \text{rank}(\mathbf{U}_F^1)$, $r_K^+ = \text{rank}(\mathbf{U}_K^+)$, $r_F^+ = \text{rank}(\mathbf{U}_F^+)$. Then we have

$$\begin{aligned} \sharp H^1(G, \mathbf{U}_K^+) &= \frac{2^n}{(\mathbf{U}_K^+ : \mathbf{U}_F^+ \cdot \mathbf{U}_K^{+1})} = \frac{2^n}{(N\mathbf{U}_K^+ : \mathbf{U}_F^{+2})} = 2 \cdot (\mathbf{U}_F^+ : N\mathbf{U}_K^+), \\ \sharp H^1(G, \mathbf{U}_K^2) &= \frac{2^n}{(\mathbf{U}_K^2 : (\mathbf{U}_K^2)^G \cdot \mathbf{U}_K^{1,2})} = \frac{2^n}{((N\mathbf{U}_K^2)^2 : ((\mathbf{U}_K^2)^G)^2)} = 2 \cdot ((\mathbf{U}_K^2)^G : (N\mathbf{U}_K^2)^2), \\ \sharp H^1(G, \mathbf{U}_K^1) &= \frac{2^{n+1}}{(\mathbf{U}_K^1 : \mathbf{U}_F \cdot \mathbf{U}_K^{+1})} = \frac{2^{n+1}}{(N\mathbf{U}_K^1 : \mathbf{U}_F^2)} = 2 \cdot (\mathbf{U}_F : N\mathbf{U}_K^1). \end{aligned}$$

Proof. By assumption, $r_F = n - 1$, $r_K = 2n - 1$. It is easy to see that $\mathbf{U}_K^+, \mathbf{U}_K^1$ and \mathbf{U}_K^2 are G -modules, and $(\mathbf{U}_K^+)^G = \mathbf{U}_F^+$, $(\mathbf{U}_K^1)^G = \mathbf{U}_F$. For $\alpha \in \mathbf{U}_K$, the norm $N_{K/\mathbb{Q}}(\alpha) = \pm 1$ (see [Nar], p.96), so $\mathbf{U}_K^2 \subset \mathbf{U}_K^1$. The following facts are also easy: $r_K^+ = r_F^+ + r_K^{+1}$, $r_K^{1,2} = r_K^{+1} = r_K - r_F = n$, $r_K^1 = r_K = 2n - 1$, $r_F^1 = r_F = n - 1$, $\mathbf{U}_F^+ \cap \mathbf{U}_K^{+1} = \mathbf{U}_K^+[2] = \{1\}$, $\mathbf{U}_F \cap \mathbf{U}_K^{+1} = \mathbf{U}_F[2] = \mathbf{U}_K^{+1}[2] = \{1, -1\}$. Then the conclusions follow directly from the above Prop.2. \square

Now again let $F, K, G, S_F, S_K, \mathbf{U}_{F,S}, \mathbf{U}_{K,S}$ be as in the above Cor.3.1.

Recall that S_F is called large for K/F if

- (i) S_F contains all ramified primes of K/F ;
- (ii) the S_K -class group of K is trivial.

Moreover, if S_F is large for K/F , and satisfies the following condition

- (iii) $G = \cup_{w \in S_K} G_w$, where G_w is the decomposition group at the place w ,

then S_F is called larger for K/F . (See [We, pp.1~2]). We denote the S_F -class group of F by $Cl_{F,S}$, which is defined to be the quotient of the ideal class group of F by the subgroup generated by the classes represented by the finite primes in S_F (see [Sa], p.127).

Proposition 3.8. If S_F is large for K/F , then the S_F -class number of F

$$h_{F,S} = \#Cl_{F,S} = \#H^1(G, \mathbf{U}_{K,S}) = 2^{\#S_K - 2\#S_F + 1} \cdot (\mathbf{U}_{F,S} : N\mathbf{U}_{K,S}),$$

so $h_{F,S}$ is a 2-power. In particular, if K/F is ramified at some finite place, and S_F is large, then

$$(\mathbf{U}_{F,S} : N\mathbf{U}_{K,S}) = 2^{2\#S_F - \#S_K - 1}.$$

Proof. By Lemma 1 of [We, p.9], we have $H^1(G, \mathbf{U}_{K,S}) \simeq Cl_{F,S}$, so by Cor.3.1 above, the first formula follows. For the second formula, by our assumption, it is obvious that S_F is also larger for K/F . By Lemma 1 of [We, p.9], the S_F -class group of F is trivial, so $\#H^1(G, \mathbf{U}_{K,S}) = 1$, which implies that $(\mathbf{U}_{F,S} : N\mathbf{U}_{K,S}) = 2^{2\#S_F - \#S_K - 1}$. \square

References

[AW] M. Atiyah, C.T.C. Wall, Cohomology of groups, in: Algebraic Number Theory (J.W.S. Cassels and A. Frohlich, Eds.), pp.94-115, London: Academic

- Press, 1967.
- [Br] K.S. Brown, Cohomology of Groups, New York: Springer-Verlag, 1982.
- [Fe] K.Q. Feng, Algebraic Number Theory (in Chinese), Beijing: Science Press, 2000.
- [IR] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, 2nd Edition, New York: Springer-Verlag, 1990.
- [JW] M.J.Jacobson,Jr, H.C.Williams, Solving the Pell Equation, CMS Books in Math., Springer, 2009.
- [Nar] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, 3rd Edition, New York: Springer-Verlag, 2004.
- [Neu] J. Neukirch, Class Field Theory, New York: Springer-Verlag, 1986.
- [Q] Derong Qiu, On quadratic twists of elliptic curves and some applications of a refined version of Yu's formula, Communications in Algebra, 42(12), 5050-5064, 2014.
- [Ro] J.J. Rotman, An Introduction to the Theory of Groups, Fourth Edition, New York: Springer-Verlag, 1995.
- [Sa] J. W. Sands, Popescu's conjecture in multi-quadratic extensions, Contemporary Math., vol.358 (2004), 127-141.
- [Se] J. -P. Serre, Local fields, New York: Springer-Verlag, 1979.

[**Wa**] L.C.Washington, Introduction to Cyclotomic Fields, 2nd Edition, New York: Springer-Verlag, 1997.

[**We**] A. Weiss, Multiplicative Galois Module Structure, AMS, Providence, Rhode Island, 1996.

[**Wei**] E. Weiss, Algebraic Number Theory, New York: McGraw-Hill Book Company, Inc, 1963.